第2版

嵌入式安全系统

产品指南

china.maximintegrated.com

maxim integrated™

目录

3 高性能、支持TFT显示的安全处理器
4 PCI PTS 3.1终端整装待发
5 独立的密码键盘加密保护SoC
6 防伪保护安全认证方案
7 高度可靠的防篡改安全管理器

利用DeepCover嵌入式安全方案提供最全面的保护

系统对安全性的要求变得愈加苛刻。随着黑客攻击手段的日趋成熟，系统所面临的风险日益加大。您的嵌入式系统需要多重保护，但是，如果没有一支专业的安全技术团队，为系统选择正确的加密保护将会面临巨大挑战。

我们的DeepCover™产品线采用专业的安全保护技术，帮助您快速整合先进的物理保护机制，为系统提供最高等级的安全防护。DeepCover嵌入式解决方案组合了三个系列的产品线，以最先进的物理保护机制满足您的应用需求。

- **DeepCover安全微控制器**采用先进的加密技术和防篡改策略，以最高安全等级应对物理篡改和逆向工程。
- **DeepCover安全认证器件**提供先进的物理保护技术，以较低成本实现超级IP保护、防克隆以及外设鉴别方案。
- **DeepCover安全管理器**采用高级物理保护和无痕存储技术，使敏感数据免受最缜密的物理攻击或篡改。

当您考虑系统安全性的时候，Maxim为您提供最可靠的保护。

高级保护、深度加密

安全性是系统设计的保障，目前，还没有任何一款片上系统(SoC) µC具备与Maxim DeepCover™安全处理器同等的安全保护级别。我们的器件集成了先进的加密和物理保护技术，提供最高等级的防物理攻击、逆向工程保护。

摆脱防护罩

可实时加密存储器的安全SoC

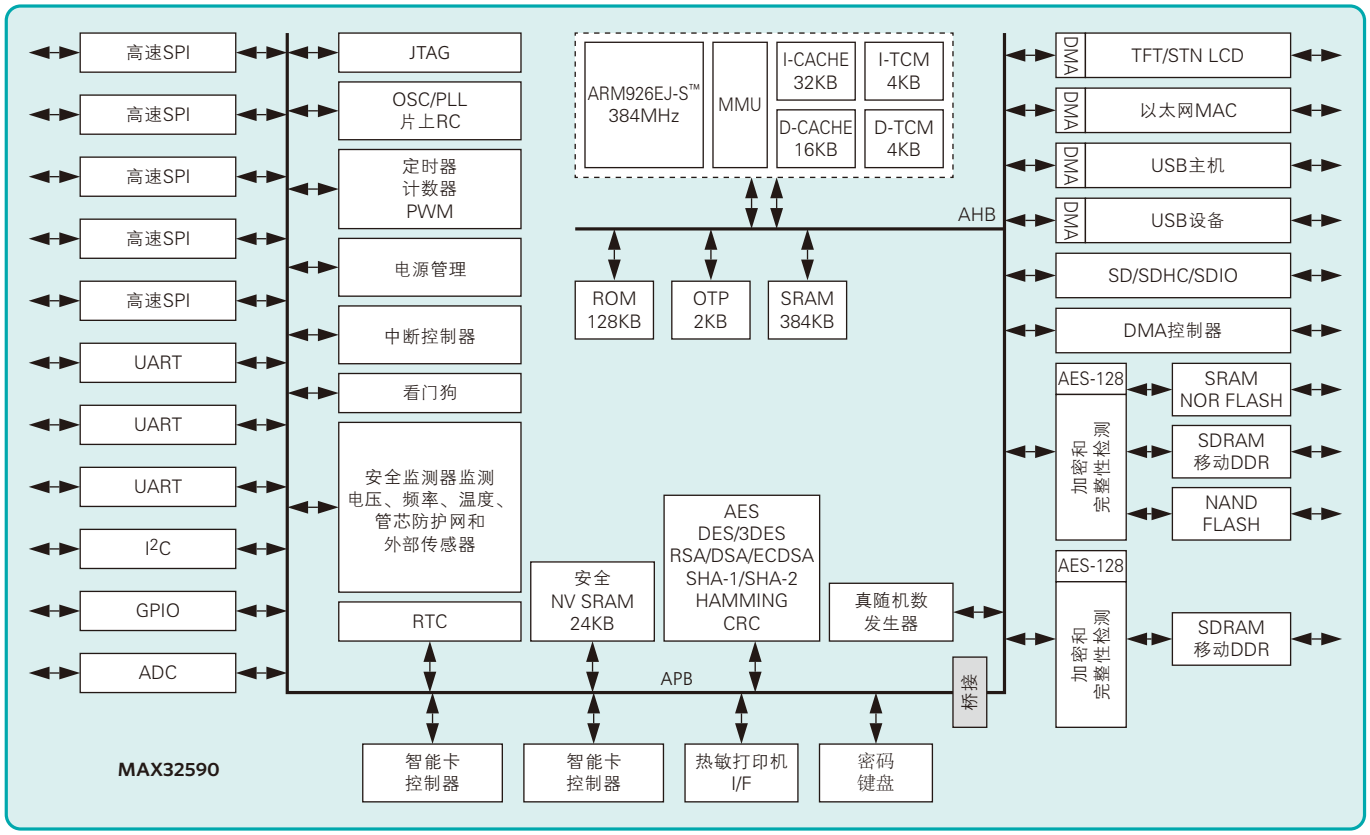
DeepCover安全微控制器(MAX32590 (JIBE))为安全、ARM9™ SoC µC，带有384MHz时钟和以太网通信接口，满足严格的金融终端安全需求。我们专有的实时加密技术能够确保您的代码安全，省去昂贵的外部防护网。全面的板级电路支持和Linux® OS支持，创新的安全机制以及高集成度设计，帮助终端产品轻松通过PCI PTS 3.1认证。利用彩色TFT显示器替代单色LCD显示器，为您的设计增添完美的视觉效果。

特性

- 完备的安全机制(经过鉴定的装载器、可立即擦除的NV SRAM、OTP、AES/SHA引擎、动态控制传感器、温度/电压/频率监测器、安全封装)
- 高级系统集成(以太网、TFT LCD、384MHz CPU、USB主机和设备)
- 实时加密外部存储器、监测信号完整性

优势

- 需要极少的外部通信控制器，降低BOM成本；彩色TFT显示器改善用户体验
- 在省去外部防护罩的同时确保最高安全性；可防止代码注入
- 简化安全设计架构，轻松通过PCI认证



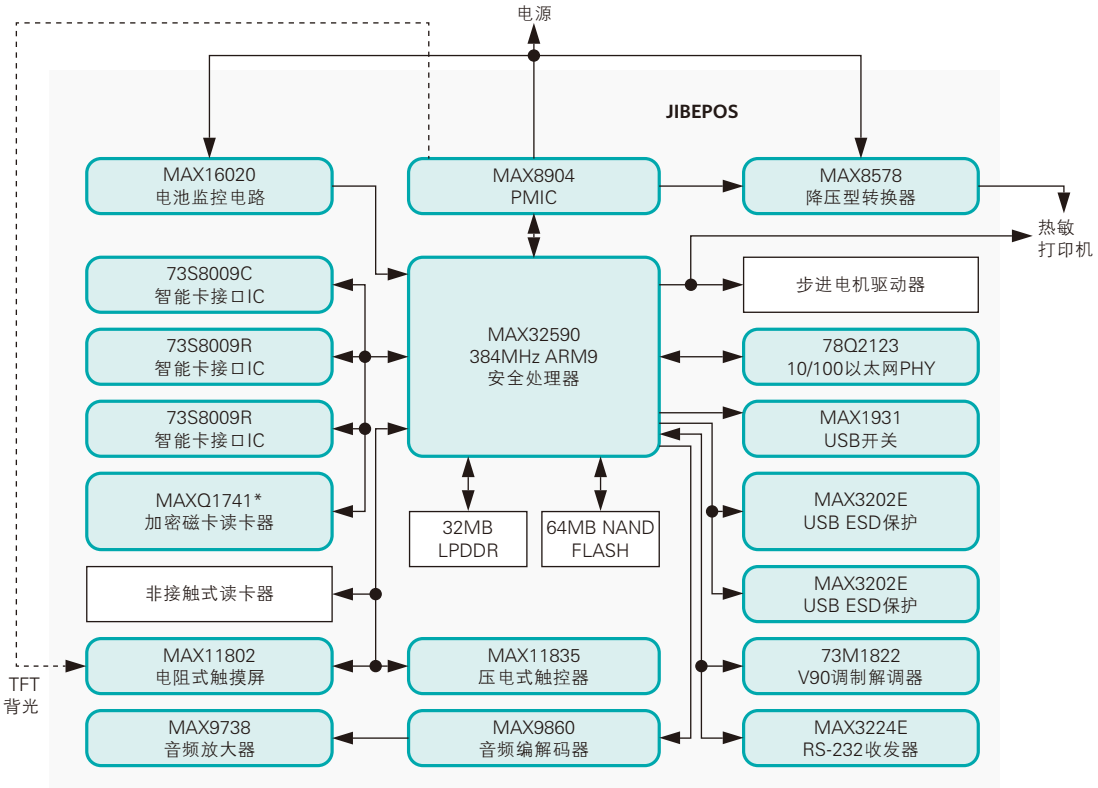
即刻获取……您的PCI PTS 3.1终端

现可提供JIBEPOS PCI PTS参考设计，缩短产品上市时间

构建您的金融终端，确保通过PCI认证。

利用功能强大的DeepCover安全微控制器(MAX32590)，我们的JIBEPOS参考设计能够使您的终端产品快速通过认证。我们提供无需外部防护罩的设计、专有的密码键盘布局、经过优化的硬件BOM、防SPA/DPA加密库、经过认证的EMV® L1库、PCI PTS兼容的安全Linux OS和安全手册，把这些资源整合到终端产品"机箱"内，轻松构建您的设计。

- 3.5英寸TFT彩色显示器
- 触觉反馈电阻式触摸屏
- 加密磁卡读卡器
- 以太网10/100、V90调制解调器、USB
- NFC非接触读卡器
- 热敏打印机
- 板载音频



从源端保护磁卡数据

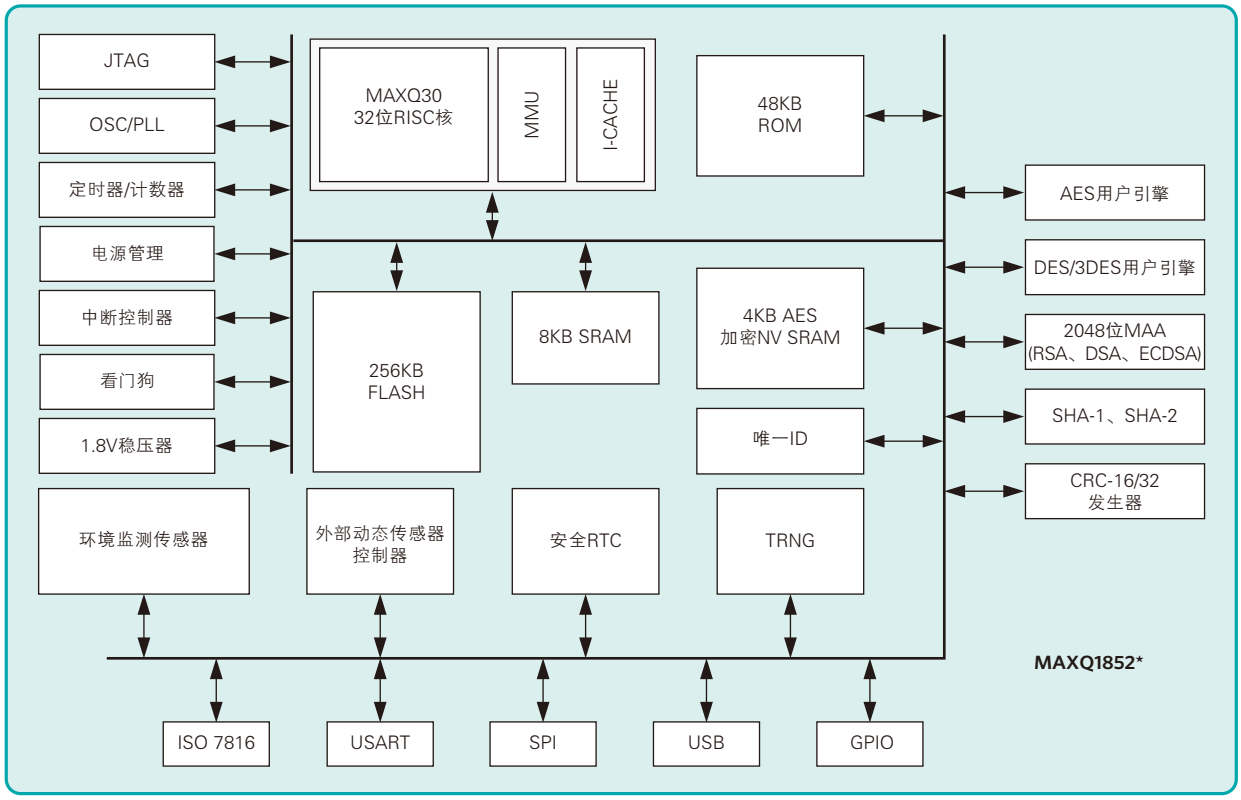
端到端加密简化设计

DeepCover安全微控制器(MAXQ1741*)将超级安全μC与高速硬件加密置于磁卡读卡器内，提供高度安全的磁卡读卡器(MSR)方案。MAXQ1741在读卡器内对敏感数据自动加密，而不是以明文发送信息。此外，器件提供便利的安全、非易失存储空间，用于存储各种安全密钥，并保护其不受物理篡改的攻击。

*未来产品——供货状况请与厂商联络。

单芯片密码键盘

DeepCover安全微控制器(MAXQ1852*)带有单指令周期的16/32位RISC处理器和对称、非对称硬件加速加密引擎，并提供ISO 7816、USB和SPI等全面的通信接口。器件可以灵活地作为一个独立控制器支持PCI-PTS 3.1密码键盘应用，也可以作为协处理器支持金融终端或其它安全应用。利用器件的GPIO引脚驱动键盘和LCD显示器，结合大容量系统SRAM和集成动态篡改侦测传感器，可进一步优化系统成本。这些动态传感器提供真正的随机信号侦测，防止旁道攻击。一旦检测到篡改操作，将立即清除内部用于加密电池备份SRAM存储内容的AES-256主密钥。器件设计还提供基于公钥(ECDSA)的加密装载器，用于内部闪存编程，使生产厂商轻松实现产品的现场升级。



安全特性

- AES、3DES、RSA、DSA、ECDSA、SHA-1、SHA-224和SHA-256硬件加密引擎
- 真正的随机数发生器(TRNG)
- 多个动态传感器输入和环境监测传感器
- 一旦检测到篡改操作，4KB AES加密NV SRAM将立即清零主密钥
- 内置稳压器支持单电源供电
- ECDSA装载器

高性能μC

- 16/32位、单指令周期RISC核
- 内部256KB闪存
- 8KB系统SRAM
- USB接口、ISO 7816控制器、RTC、USART、SPI总线
- 68引脚TQFN或64焊球CSBGA封装

*未来产品——供货状况请与厂商联络。

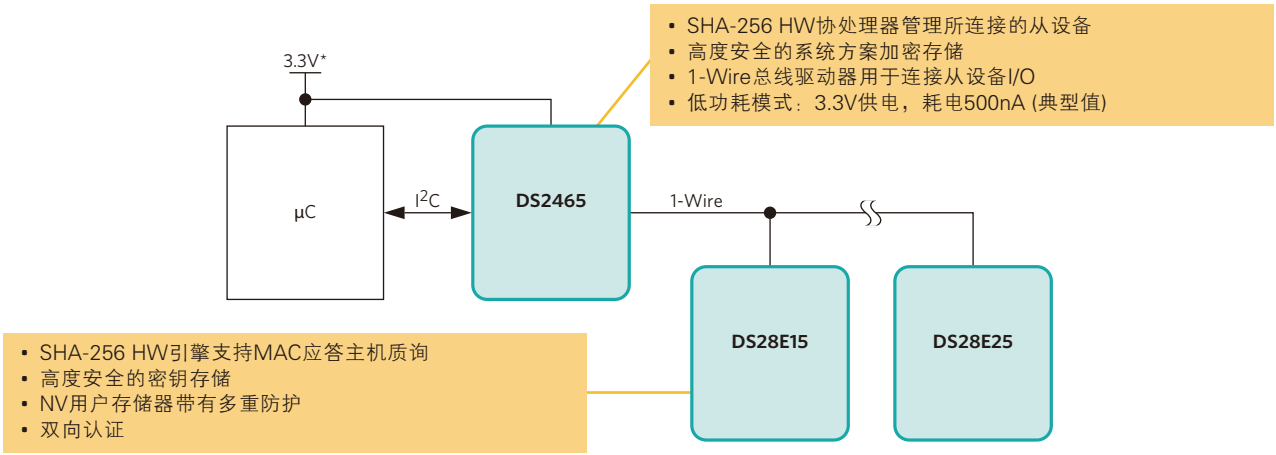
杜绝造假者窃取您的IP

研发成果是您的最大财富，需要采取可靠的保护措施杜绝那些生产或销售您的产品的假冒行为。我们的DeepCover™安全认证方案采用先进的物理保护机制，以较低成本提供终极IP保护、防克隆及外设授权监测等方案。从安全保护、密钥管理、基于FIPS 180的质询–应答双向认证，到用户定制的唯一64位、工厂刻制序列号，我们提供完备的产品支持。

- OEM认证
- 系统防克隆保护
- HW/SW授权管理
- 篡改监测配置
- 安全/品质担保

型号	说明	主机接口	认证特性
DS2465	SHA-256协处理器，带有1-Wire®主机	I²C	系统加密安全存储器
DS28E15，DS28E22，DS28E25	SHA-256，0.5Kb/2Kb/4Kb EEPROM	1-Wire	双向质询–应答
DS28CN01	SHA-1，1Kb EEPROM	I²C/SMBus	双向质询–应答
DS28E01-100，DS28E02	SHA-1，1Kb EEPROM	1-Wire	双向质询–应答
DS28E10	SHA-1，224b OTP EEPROM	1-Wire	质询–应答
DS2460	SHA-1协处理器	I²C	系统加密安全存储器
MAX66040，MAX66140	SHA-1，1Kb EEPROM	RF	双向质询–应答，ISO 14443B/15693
DS2431	1Kb EEPROM	1-Wire	定制64位ROM、WP/OTP模式
DS2401，DS2411	64位ROM序列号	1-Wire	定制64位ROM

SHA-256新型产品轻松应对主、从设备设计挑战



*如需1.8V方案，请与厂商联络。

轻松增添系统安全功能

DeepCover安全管理器提供完备的硬件加密，无需重新设计系统

Maxim Integrated全面的DeepCover™安全管理器允许用户在其现有的系统处理器上轻松添加先进的物理安全功能。这些IC采用专有的“无痕”存储器存储关键数据，一旦侦测到篡改事件将立即擦除存储器内容。无论系统是否供电，安全管理器将连续监测篡改操作。

- 配合现有的微处理器工作
  - 提供I²C或SPI接口
- 内置安全存储器
  - 无痕存储器
  - 64B至4KB存储容量
- 内置篡改监测器
  - 温度(包括温度变化率)
  - 功耗
  - 振荡器
- 监测外部电路，避免篡改攻击
- 实时时钟/计数器
  - 提供篡改事件时标
- 小尺寸CSBGA封装
- 电池备份期间处于低功耗模式
- 主电源监测
  - 自动从主电源切换到电池
- 提供外部SRAM供电和擦除控制

具有防篡改和无痕存储器的硬件AES加密方案，为您提供业内最高等级的安全防护

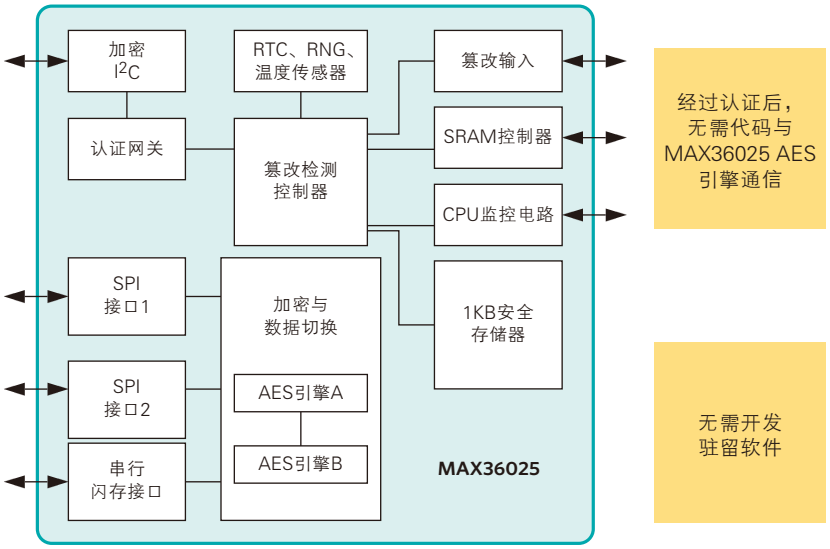
DeepCover安全管理器(MAX36025)具有硬件加密和市场上最先进的防篡改功能。利用MAX36025对数据进行硬件加密/解密，其安全等级远远高于通用微处理器的软件加密方案。由于密钥从不离开MAX36025芯片，在防篡改电路的保护下，使其更加安全可靠。

通用特性

- 双AES处理器
  - 支持128、192和256位密钥
  - ECB、CTR和CBC模式
- 通过加密的I²C接口进行认证
- 双向SPI接口
  - 采用同一密钥加密/解密数据
  - 支持独立的加密/解密数据流

安全特性

- 1KB无痕存储器用于密钥存储
  - 段存储器用于存储两组关键数据
- 温度、功耗和振荡器篡改监测器
- 数字和模拟输入篡改监测



安全微控制器

型号	速度与核	内部闪存/SRAM储器(KB)	安全NV SRAM (KB)	外部存储器	USB†	SPI	ISO 7816	GPIO	电池电流(µA)	封装
MAXQ1004	6MHz，MAXQ20	16/640B	—	—	—	1	—	8	300nA	16-TQFN
MAXQ1010	12MHz，MAXQ20	128/2	128B	—	D	1	1	31	400nA	48-TQFN
MAXQ1011*，MAXQ1012*	12MHz，MAXQ20	64，32/1	128B	—	D	1	1	31	400nA	48-TQFN
MAXQ1050	25MHz，MAXQ20	128/12	256B + 4KB AES加密	—	D	1	1	20	240nA	40-TQFN
MAXQ1740，MAXQ1741*	12MHz，MAXQ20	16/—	1152B	—	—	2	—	16	3	28-TQFN
MAXQ1850	16MHz，MAXQ30	256/—	8	—	D	1	单(双卡)	16	130nA	40-TQFN，49-CSBGA
MAXQ1851*	16MHz，MAXQ30	256/8	256位 + 4KB AES加密	—	D	1	单(双卡)	16	350nA	40-TQFN，49-CSBGA
MAXQ1852*	16MHz，MAXQ30	256/8	256位 + 4KB AES加密	—	D	1	单(双卡)	32	350nA	68-TQFN，64-CSBGA
USIP	96MHz，MIPS32® 4KSd™	256/128	512位	NOR flash，SRAM，SDRAM	O	1	3	32	2.9	256-CSBGA
ZA9L0	180MHz，ARM922T	—/64	4	NOR flash，SRAM，SDRAM	—	1	2	76	21	256-CSBGA
MAX32580*	192MHz，ARM926EJ-S	—/384	256位 + 24KB AES加密	—	D	2	2	129	6	169-CSBGA
MAX32590	384MHz，ARM926EJ-S	—/384	256位 + 24KB AES加密	NOR flash，NAND SRAM，SDRAM LPDDR	D，H	5	2	160	6	324-LFBGA

†D = 设备端口；O = OTG端口；H = 主机端口

安全管理器

型号	温度范围(°C)	功耗(典型值)(µA)	无痕存储器(KB)	外部篡改监测	I/O	认证	AES加密ECB/CTR/CBC模式	评估板	封装
DS3600，DS3605	-40至+85	5.7	64B (DS3600)	4	3线/I²C	—	—	✓ (DS3600)	25-CSBGA
DS3640，DS3641	-40至+85	6.5	1	4	4线/I²C	—	—	✓	25-CSBGA
DS3645	-55至+95	12	4	8	I²C	—	—	✓	49-CSBGA
DS3650，MAX36051	-40至+85	3.0，1.5	128B	2	4线	—	—	✓ (MAX36051)	16-CSBGA
MAX36025	-55至+95	9	1	8	SPI (2)	加密I²C	2 AES引擎	✓	81-CSBGA

*未来产品——供货状况请与厂商联络。

DeepCover和1-Wire分别是Maxim Integrated Products, Inc.的商标和注册商标。
ARM9和ARM926EJ-S是ARM Limited的商标。
EMV是EMVCo LLC.的注册商标。
Linux是Linus Torvalds的注册商标。
MIPS32和4KSd分别是MIPS Technologies, Inc.的注册商标和商标。

如需获取更多信息，请访问：china.maximintegrated.com。
技术支持：800-810-0310 (免费电话)或010-6211 5199 • eMail：AP.Support@maximintegrated.com

© 2012 Maxim Integrated Products, Inc.版权所有。Maxim Integrated和Maxim Integrated标志是Maxim Integrated Products, Inc.在美国及其他管辖区域的商标。其他公司名称为相应公司的注册商标名或商标。

Rev. 1; 2012年11月